

Amendments to the Claims

1-10. (canceled)

11. (currently amended) A computer program product for use with a client-server computer network, the network comprising a set of server computers and a set of client computers, said computer program product comprising a computer usable medium having computer readable program code ~~means~~ embodied in said medium for providing authentication of cookies, said computer program product comprising:

- a. computer readable program code ~~means for enabling a first~~ operative to enable one or more of the set of client computers ~~communicating with a first one of the set of server computers to provide~~ client-identifying data to the first one or more of the set of server computers,
- b. computer readable program code ~~means for enabling the first~~ operative to provide a unique server-identifier for each one of the set of server computers ~~to request a private key and an associated public key from a public encryption system,~~
- c. computer readable program code ~~means for causing the first~~ operative to enable each one of the set of server computers to ~~maintain the~~ request a private key in a dynamic memory device and an associated public key from a public key encryption system,

d. computer readable program code ~~means for causing the first~~ operative to enable each one of the set of server computers to maintain store the public-requested private key in a database available to the set of server computers, dynamic memory device on the server computer, only,

e. computer readable program code ~~means for enabling the first~~ operative to enable each one of the set of server computers to generate a cookie for the first one of store the requested public key in a database available to the set of client computers, the cookie comprising data corresponding to the identifying data provided by the first one of the set of client computers server computers, and to associate the stored public key requested by the server computer with the unique server-identifier for the server computer,

f. computer readable program code ~~means for causing the first~~ operative to enable each one of the set of server computers to generate a digital signature for the cookie, cookies for one or more of the set of client computers, each generated cookie comprising data corresponding to the client-identifying data provided by the one or more of the set of client computers and comprising the value of the server-identifier assigned to the generating server,

g. computer readable program code ~~means for causing the first~~ operative to enable each one of the set of server computers to encrypt the generate an encrypted digital

signature for each generated cookie using the ~~public key encryption system and the~~
requested private key stored in dynamic memory on the server computer,

h. computer readable program code ~~means for enabling the first~~ operative to enable
each one of the set of server computers to forward ~~the cookie cookies~~ and ~~the their~~
associated encrypted digital ~~signature~~ signatures to the ~~first one of the set of~~ client
computers corresponding to the identifying data provided,

i. computer readable program code ~~means for enabling the first one of the set of~~
~~client computers to communicate with a second one of the set of server computers, and in~~
~~response, the second one of the set of server computers to request and receive the cookie~~
~~and the encrypted digital signature from the first~~ operative to enable each one of the set of
server computers to receive cookies with encrypted digital signatures from one or more
of the set of client computers, and

j. computer readable ~~computer program~~ code ~~means for causing the second~~
~~operative to enable each~~ one of the set of server computers to extract server-identifying
data from received cookies to retrieve ~~the public key for the encrypted digital signature~~
~~from the database and to decrypt the digital signature using the public key encryption~~
~~system and the retrieved public key, and~~ k. computer readable program code means for
enabling the second one of the set of server computers to use the decrypted digital
signature to authenticate the cookie received from the first one of the set of client

~~computers~~ associated public keys from the database for use in decrypting digital signatures for received cookies and thereby to authenticate the said cookies.

12. (currently amended) The computer program product of claim 11, further comprising:
- a. ~~computer readable program code means for assigning a unique server identifier to each responsive to the restart of a one of the set of server computers,~~
 - b. ~~computer readable program code means for associating a corresponding server identifier with each public key maintained in the database, and~~ and operative to request a replacement private key and an associated replacement public key,

computer readable program code operative to cause the replacement private key to be stored in the dynamic memory of the server computer, and

e. ~~computer readable program code means for retrieving~~ operative to cause the replacement public keys key to be stored in the database by reference to a server identifier.

13. (currently amended) The computer program product of claim ~~11~~ 12, further comprising
- ~~computer readable program code means for removing one or more public keys from the database when the one or more public keys have been maintained~~ operative to cause the deletion of public keys in the database where such keys have been stored for longer than a preselected predetermined elapsed time.

14. (currently amended) A method for providing authentication of cookies in a client-server computer network, the network comprising a set of server computers and a set of client computers, each one of the set of server computers having a unique server-identifier, the method comprising the following steps:

- a. a first one of the set of client computers ~~communicating with~~ providing client-identifying data to a first one of the set of server computers, ~~the first one of the set of client computers providing identifying data to the first one of the set of server computers,~~
- b. the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system,
- c. the first one of the set of server computers ~~maintaining~~ storing the requested private key in a dynamic memory device; on the first server computer, only,
- d. the first one of the set of server computers ~~maintaining~~ causing the requested public key to be stored in a database available to each one of the set of server computers, and to associate the stored public key with the unique server-identifier for the first one of the set of server computers,

e. the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the client-identifying data provided by the first one of the set of client computers, and comprising the value of the server-identifier for the first one of the set of server computers,

f. the first one of the set of server computers generating a an encrypted digital signature for the cookie using the private key stored in dynamic memory of the first one of the set of server computers,

g. the first one of the set of server computers ~~encrypting the~~ forwarding the cookie including the associated encrypted digital signature ~~using the public key encryption system and the private key~~ to the first one of the set of client computers,

h. the first one of the set of ~~server computers forwarding the cookie and the associated~~ client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie including the encrypted digital signature to ~~from~~ the first one of the set of client computers,

i. ~~the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie and the encrypted digital signature from~~

~~the first one of the set of client computers, j. the second one of the set of server computers extracting server-identifying data from the received cookie to retrieve the associated public key for the encrypted digital signature from the database and for use in decrypting the digital signature using the public key encryption system and the retrieved public key, k. the second one of the set of server computers using the decrypted digital signature to authenticate the cookie received from the first one of the set of client computers.~~ for the received cookie and thereby authenticating the cookie.

15. (currently amended) The method of claim 14 comprising the further steps of:

a. ~~assigning a unique server identifier to each~~ the first one of the set of server computers; b. ~~associating a corresponding server identifier with each public key maintained in the database, and~~ c. ~~retrieving public keys in the database by reference to a server identifier.~~ requesting a replacement private key and an associated replacement public key in response to a restart,

storing the replacement private key in the dynamic memory of the server computer, and

storing the replacement public key in the database.

16. (currently amended) The method of claim 14 comprising the further step of ~~removing one or more~~ deleting public keys from the database when the one or more public keys have been

~~maintained~~ in the database where such keys have been stored for longer than a ~~preselected~~
predetermined elapsed time.